The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/13/2012
7/10/2012 - UPDATED

SUBJECT: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS12-043)

ORIGINAL OVERVIEW:
A vulnerability has been discovered in the Microsoft Core XML Services (MSXML) which could allow an attacker to take complete control of an affected system. MicrosoftCore XML Services is software which allows users to develop XML based applications. This vulnerability can be exploited if a user with a vulnerable MSXML package visits or is redirected to a malicious web page using Microsoft Internet Explorer. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability at this time and Microsoft has reported that this vulnerability is actively being exploited in the wild.

July 10 – UPDATED OVERVIEW:
Microsoft has released a patch that fixes this vulnerability in security bulletin MS12-043.

SYSTEMS AFFECTED:
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft XML Core Services (MSXML) 6.x and earlier

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

ORIGINAL DESCRIPTION:
A vulnerability has been discovered in the Microsoft Core XML Services 3.0, 4.0, 5.0, and 6.0 which could allow an attacker to take complete control of an affected system. This vulnerability exists because MSXML attempts to access an object in memory that has not been initialized resulting in potential memory corruption. To exploit this vulnerability, an attacker creates a specially crafted website and entices users to visit that site through e-mail or by some other means. Successful exploitation could occur if the site is visited by a user running Internet Explorer and has MSXML versions 3.0, 4.0, 5.0, or 6.0 installed.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability at this time and Microsoft has reported that this vulnerability is actively being exploited in the wild.

July 10 – UPDATED DESCRIPTION:
Microsoft has released a patch that fixes this vulnerability in security bulletin MS12-043.

ORIGINAL RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems as soon as they are available after testing.
- Consider implementing one or more of the following workarounds recommended by Microsoft:
    - Implement the workaround described in Microsoft Knowledge Base article 2719615. (http://support.microsoft.com/kb/2719615)
    - Consider configuring the Enhanced Mitigation Experience Toolkit (EMET) for Internet Explorer to temporarily mitigate this vulnerability.
    - Run Internet Explorer in a restricted mode to temporarily mitigate this vulnerability. This is the default setting on Windows Server 2003 and 2008. (http://technet.microsoft.com/en-us/library/dd883248(WS.10).aspx)
    - Configure Internet Explorer to prompt before running Active Scripting or disable Active Scripting to temporarily mitigate this vulnerability.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

July 10 – UPDATED RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems after testing**.**

ORIGINAL REFERENCES:
Microsoft:
http://technet.microsoft.com/en-us/security/advisory/2719615
http://support.microsoft.com/kb/2719615
http://technet.microsoft.com/en-us/library/dd883248(WS.10).aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889
Security Focus:
http://www.securityfocus.com/bid/53934

Secunia:
http://secunia.com/advisories/49456

July 10 – UPDATED REFERENCES:
Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/MS12-043
http://technet.microsoft.com/en-us/security/advisory/2719615